GENERAL-PURPOSE SECURE ANONYMITY ARCHITECTURE

Gergely TÓTH
Advisors: Zoltán HORNÁK, Ferenc VAJDA

I. Introduction

The rapid development in the area of computer science, hardware, software and communication systems made it possible to integrate information systems in a constantly increasing factor. This tendency together with the spreading of Internet sets newer and newer challenges for the information science. For the first problems of bandwidth and reliable data transfer several general architectural solutions exist. However nowadays new needs arise: besides the given features *secure* communication is also required. In the field of encryption, integrity-protection or non-repudiation honored solutions are already known (such as SSL), but their integration with anonymity methods is neither complete nor standardized.

The latest development brought the protection of personal data — *privacy* — into the spotlight. As larger and larger databases get connected and made — partially publicly — searchable, more and more information about people can be collected. As a sort of countermeasure, anonymity is required in order to hide the identity.

For providing anonymity several different techniques exist. But we lack their uniformity and the means of integrating them into a general system. They can basically be grouped into two categories:

- *Anonymous handshaking schemes*: with the help of an anonymity authority they make possible for a service provider to be certain that an anonymous subject is authorized to use a specified service. Typical application areas are: anonymous electronic payment (subject is the client, anonymity authority is the bank and the authorization is the payment) [1] or anonymous electronic voting (subject is the voter, anonymity authority is the issuer of the ballot and the service provider is the electronic ballot-box). Anonymous transport is required in the most cases for the anonymous authorization to work properly.
- *Anonymous transport methods*: in the communication between the subject and the service provider they make the subject's location anonymous, thus he cannot be traced back. Typical applications are anonymous electronic mailing [2] or anonymous on-line web-surfing [3].

II. Requirements

An architecture is needed that provides security functions, guarantees the anonymity of the subject and incorporates a general framework for the usage of anonymous authorization schemes. These three aspects have to be easily employable from the application layer. An important restriction is that by moving to this new architecture existing applications should need the least possible level of modification. Optimally existing applications should be able to use the new architecture without modifications.

III. Architecture

A. Aim

In the field of anonymity we lack a framework that incorporates all required aspects. The general-purpose secure anonymity architecture aims to address this problem by providing an environment, where different anonymity techniques can be implemented and scientifically analyzed.

B. Description

A general-purpose secure anonymity architecture (see Figure 1) answering the requirements above was designed with the considerations below in mind:

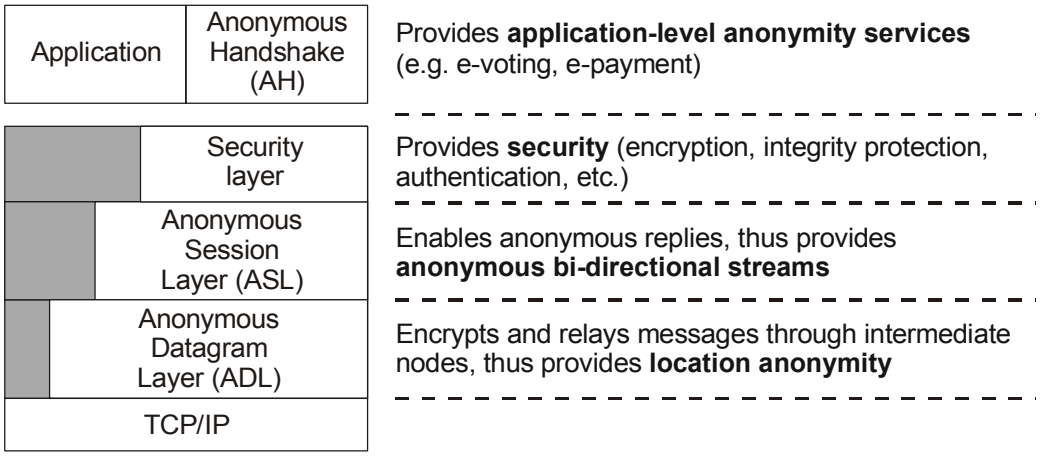

Figure 1: General-purpose secure anonymity architecture

The standard TCP/IP protocol of the Internet was used for data transmission. However, since between the user and the service provider no direct TCP/IP connection may exist (from the IP address the user could become back-traceable) the *Anonymous Datagram Layer* (ADL) has to be introduced. The purpose of this layer is to ensure that messages sent by a user cannot be linked to him. This is achieved by introducing several relay nodes in the network, which mix and encrypt messages of several different users (with the help of cryptographic algorithms) and thus obfuscate the traffic.

In order to enable stream connection between the user and the service-provider, thus making it possible for the service provider to address the user even though it does not know his address, the *Anonymous Session Layer* (ASL) has to be introduced into the hierarchy.

On top of ADL and ASL a standard *security layer can* be inserted. Since several anonymity scenarios (electronic voting or on-line payment) require confidentiality, integrity or non-repudiation, one of the commonly used security layers (such as SSL or TLS) should be used.

Finally Anonymous Handshake is introduced in order to realize the anonymous authorization. For this purpose AEP (Anonymity Enhancing Protocol, [4]) can be used.

The architecture defines solely requirements and the service primitives (thus the functionality) for the layers mentioned above, several different techniques and protocols could be used for the implementation.

IV. Conclusion

The general-purpose secure anonymity architecture incorporates both security features (such as confidentiality, integrity or authentication) and anonymity measures (for transparent anonymous communication and authorization).

References

[1] D. Chaum: *Blind Unanticipated Signature Systems*, U.S.Patent 4 759 064, 1998.

[2] D. Chaum.: *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*, Communications of the ACM, volume 24, number 2, pp. 84-88, 1981.

[3] *Anonymizer.com – Online Privacy Services*, http://www.anonymizer.com

[4] G. Tóth: *Anonymity Enhancing Protocol*, Ms.E. thesis., Siemens-Award 2002.

[5] G. Tóth, Z. Hornák: *Measuring Anonymity*, IWCIT'03